Komunikacija između procesa (pitanja za provjeru znanja)

1. Navesti mehanizme za međusobnu komunikaciju između procesa na jednom računalu.
    1. Razmjena datoteka (statička komunikacija)
    2. Zajednička uporaba izvornih podataka u dijeljenom spremničkom prostoru (dinamička komunikacija)
    3. Uporaba kopija podataka zasnovana na razmjeni poruka (dinamička komunikacija)
    4. Cjevovodi (nije u knjizi – obrađeno na labosu)
    5. Varijable okoline (nije u knjizi – obrađeno na labosu)
2. Kako mogu komunicirati procesi na udaljenim računalima
    1. Razmjenom poruka
    2. Poziv udaljenih procedura
    3. Raspodijeljeni dijeljeni spremnički prostor
3. Opisati mehanizme poziva udaljenih procedura (RPC)
    - Slično kao pozivi potprograma, ali se instrukcije procedure ne nalaze u istom adresnom prostoru kao pozivatelj pa pozivatelj i proces gdje je procedura moraju razmjeniti ulazne podatke i rezultate – razmjena poruka (nisu u istom adr. prostoru pa mora ići „call by value“) . Ostvaren je iznad TCP razine tako da poziv udaljene procedure izgleda kao uobičajeni poziv potprograma, ali postoji spojni modul koji radi konverziju između procesa i TCPa. Kod primatelja isto tako.
4. Navesti mehanizme koji omogućuju međusobno isključivanje dretvi i procesa na jednom računalu.
    1. Zabranom prekidanja (dretva kada ide u KO zabrani da ju se prekine) – kod jednoprocesorskih sustava – semafori i monitori
    2. Nedjeljivim čitanjem i pisanjem (ispitivanje zastavice u zajedničkom prostoru) – kod višeprocesorskih sustava
5. Opisati centralizirani protokol međusobnog isključivanja u raspodijeljenim sustavima.
    - Jedan od čvorova je odgovoran za međusobno isključivanje. On raspolaže sa svime i ostali moraju od njega tražiti dozvolu za ulazak u KO tako da mu pošalju zahtjev. Kada budu mogli ići u KO centralni čvor će im poslati odgovor do tada čekaju. Kada izađu iz KO moraju to javiti centralnom čvoru koji onda pušta idućeg u redu za čekanje. Red je organiziran po vremenu dospjeća.
6. Opisati protokol s putujućom značkom.
    - Definira se značka. Ona ciklički putuje kao poruka između čvorova. Ako želi pristupiti u KO, proces čeka da dobije značku te onda ulazi u KO, po izlasku iz KO šalje značku dalje.
7. Opisati lokalni i globalni logički sat.
    - Lokalni logički sat – brojač, svaki proces ga može imati. Povećava svoju vrijednost nakon svakog karakterističnog događaja unutar procesa
    - Globalni logički sat – skup pravila vremenskog uređenja na razini sustava. Proces povećava svoj logički sat nakon svakog svog događaja. Proces šalje vrijednost svog logičkog sata uz svaku poruku. Proces koji primi poruku uspoređuje svoj logički sat s vrijednošću sata iz poruke i postavlja svoj logički sat na veću vrijednost od te dvije + 1.

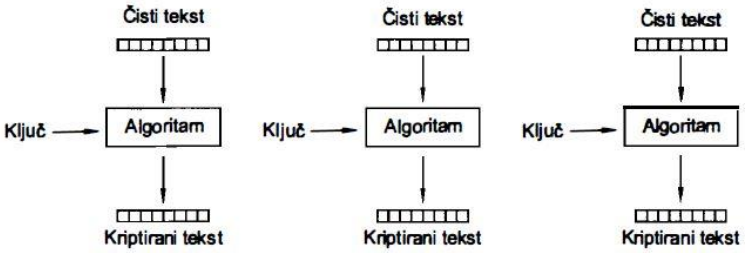
8. Opisati raspodijeljeni Lamportov protokol
   - Zasniva se na uvažavanju vremenskog uređenja temeljenog na globalnom logičkom satu. Svaki proces ima red poruka za zahtjeve za ulazak u KO. Pet pravila za funkcioniranje protokola
     a) Kada Pi želi u KO mora poslati poruku zahtjev(i, Ci) i staviti istu poruku u svoj red čekanja.
     b) Kada Pj primi zahtjev(i, Ci) on mora uskladiti svoj lokani sat (po pravilima uspostave globalnog sata), staviti u red čekanja zahtjev(i,Ci) i poslati poruku odgovor(i,**Cj**) procesu Pi
     c) Pi smije uću u KO kada je njegov zahtjev na početku reda i kada je primio poruke odgovora od svih ostalih procesa
     d) Pi nakon izlaska iz KO uklanja svoj zahtjev iz reda i šalje svima poruku izlazak(i,Ci). Ci u poruci je jednak onom iz reda čekanja.
     e) Kada Pj primi izlazak(i,Ci) miče i-ov zahtjev iz reda čekanja
   - Za ulazak i izlazak iz KO razmijeni se 3*(N-1) poruka
9. Objasniti protokol Ricarta i Agrawala.
   - Odgovore na primljenje poruke šalju samo kada ustanove da ne žele ući u KO ili da proces koji je poslao zahtjev ima pravo prvenstva. Pravila:
     a) Kada Pi hoće u KO šalje zahtjev(i,Ci) svima
     b) Kada Pj primi poruku zahtjev(i,Ci) on mora uskladiti svoj lokalni sat, poslati odgovor(**j**,Ci) ako ne želi u KO ili ako je zahtjev Pi-a došao ranije
     c) Kada Pi primi odgovore od svih procesa smije ući u KO
     d) Nakon izlaska iz KO Pi šalje poruku odgovor(j,Ci) svim procesima čiji zahtjevi čekaju kod njega na odgovor
   - Za ulazak i izlazak iz KO razmijeni se 2*(N-1) poruka

Sigurnost računalnih sustava (pitanja za provjeru znanja)

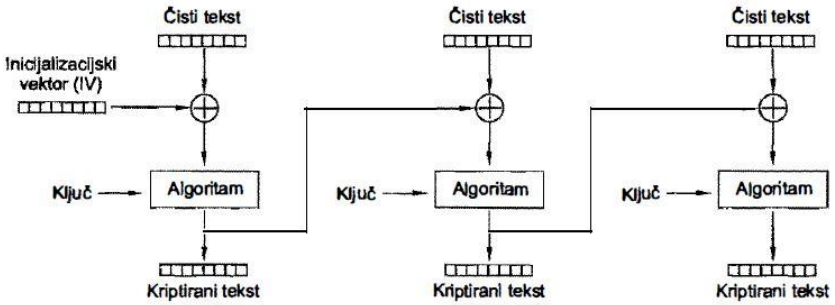
1. Objasniti pojmove identifikacija, autentifikacija i autorizacija.
   - Identifikacija – predstavljanje korisnika računalu
   - Autentifikacija – postupak provjere identifikacija (provodi računalo)
   - Autorizacija – mehanizmi dopuštanja pristupa pojedinim sredstvima
2. Navesti vrste napada na sigurnost računalnog sustava
   - Prisluškivanje (jedini pasivni napad, ostali su aktivni)
   - Prekidanje
   - Promjena sadržaja poruka
   - Izmišljanje poruka
   - Lažno predstavljanje
   - Poricanje
3. Navesti sigurnosne zahtjeve
   - Povjerljivost ili tajnost
   - Raspoloživost
   - Besprijekornost ili integritet

- Autentičnost
- Autorizacija
- Neporecivost

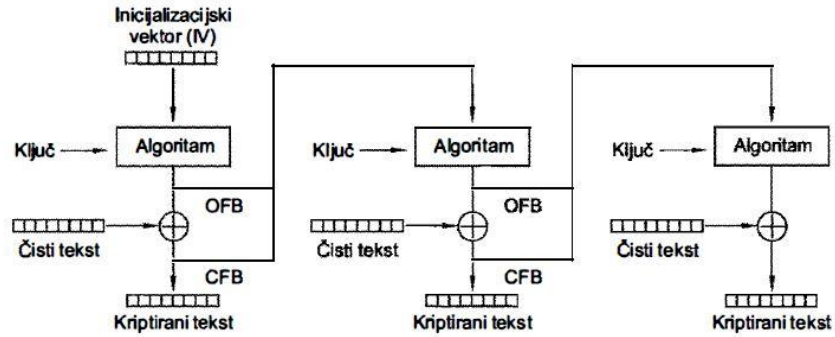
4. Navesti svojstva simetričnog i asimetričnog kriptosustava
   - Simetrični – ključ kriptiranja je jednak ključu dekriptiranja
   - Asimentrični – ima različite ključeve za kriptiranje i dekriptiranje
5. Na koji način se kriptira jasni tekst M koristeći jednokratnu bilježnicu (one time pad)?
   - Simetrični, XOR teksta s ključem, kao ključ se koristi neki dogovoreni tekst (random generiran) i iste veličine kao poruka koja se kriptira. Za svaku poruku se generira novi ključ. NAJSIGURNIJI ALGORITAM –matematički dokazano, ako se poštiva ovo gore navedno - što je teško ispuniti
6. Navesti nekoliko simetričnih kriptosustava.
   - Jednokratna bilježnica, DES, 3DES, DESX, IDEA, AES
7. Koje su moguće duljine ključeva u kriptosustavima DES, IDEA i AES?
   - DES – 56 bitova (blok 64 bita)
   - IDEA – 128 bitova (blok od 64 bita)
   - AES – 128, 192 i 256 bita (blok od min 128 bita)
8. Navesti postupak kriptiranja i dekriptiranja utrostručenim DES kriptosustavom.
   - trostruko DES kriptiranje (jedno za drugim: DES -> DES^-1 ->DES), upotrebljava se 3 ključa duljine 56 bita (ukupno |K|=168bita). Dekriptiranje je samo 3 puta nazad (DES^-1 -> DES -> DES^-1)
9. Navesti postupak kriptiranja i dekriptiranja izbijeljenim DES kriptosustavom.
   - Uz 56 bitni K upotrebljavaju se još dva 64 bitna ključa (K2, K3) koji izbjeljuju dijelove teksta. Prvo se XORa s jednim dodatnim ključem (K2), pa DES s K pa opet XOR s dodatnim (K3). Dekriptiranje je samo naopačke (XOR s K3, DES^-1 s K, XOR s K2)
10. Čemu služe supstitucijske (S) tablice u kriptosustavima DES i AES?
    - Za zamjenu znakova, dodatna zaštita (nije dovoljno precizno jer Petra da neće doć takvo sranje)
11. Skicirati ECB, CBC, CFB, OFB i CTR načine kriptiranja.



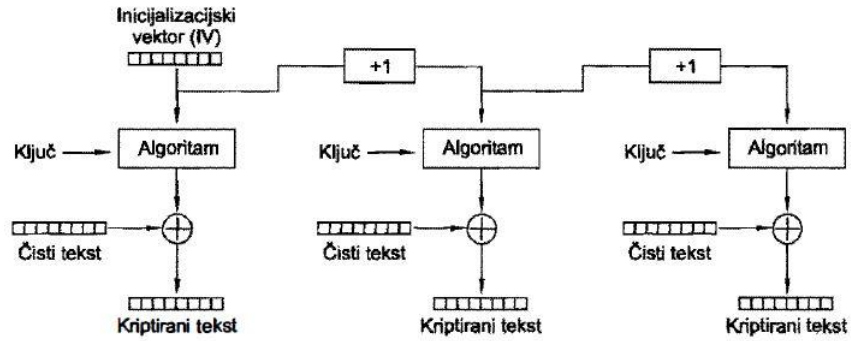
Slika 11.15. Kriptiranje u ECB načinu



Slika 11.17. Kriptiranje ulančavanjem (CBC)



Slika 11.19. CFB i OFB načini kriptiranja



Slika 11.20. CTR način kriptiranja

12. Koji je osnovni nedostatak ECB načina kriptiranja?
    - Svaki blok se kriptira (dekriptira) neovisno o ostalim blokovima pa je teško napraviti dobro kriptiranje neovisno o jačini algoritma za kriptiranje
13. Koji su načini kriptiranja pogodni za kriptiranje toka podataka?
    - CFB, OFB i CTR